IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

Claims 1-8 (canceled).

9. (currently amended)A symmetric-key decryption method performed by a computer, comprising the steps of:

dividing ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

~~generating a random number sequence based on a secret key;~~

generating a first random number block and a second random number block both corresponding to each ~~one~~ of said plurality of ciphertext blocks based on a secret key that is an input value~~from said random number sequence~~;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating the series of said ciphertext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the ciphertext obtained from the plaintext has been altered,

wherein one of said decryption operations for producing the plaintext block i corresponding to the ciphertext block i (2 <i< a number of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number of said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

~~outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back for use in the operation on another one of the plurality of ciphertext blocks; and~~

~~performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.~~

10. (currently amended)The symmetric-key decryption method as claimed in claim 9, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said ciphertext blocks~~said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks~~.

11. (original) The symmetric-key decryption method as claimed in claim 10, further comprising steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

12. (currently amended)The symmetric-key decryption method as claimed in claim 11, further comprising steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claims 13-20 (canceled).

21. (currently amended)A symmetric-key decryption apparatus comprising:

a circuit for ~~receiving~~ dividing ciphertext, which is an input text, ~~and dividing the received ciphertext~~ to generate a plurality of ciphertext blocks each having a predetermined length;

a random number generation circuit for ~~receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and~~ generating a first random number block and a second random number block both corresponding to each ~~one~~ of said plurality of ciphertext blocks based on a secret key that is an input value~~from said random number sequence~~;

a decryption operation circuit for performing decryption operations to produce plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

a circuit for concatenating the series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

a circuit for examining the redundancy data to detect whether the ciphertext obtained from plaintext has been altered,

wherein said decryption operation circuit for producing the plaintext block i corresponding to the ciphertext block i (2 <i< a number of ciphertext blocks) comprises:

a first circuit for performing a first operation on said ciphertext block i,

a second circuit for performing a second operation on a result of said first

operation performed on said ciphertext block i and said first random block corresponding to said ciphertext block i, and

a third circuit for performing a third operation on a result of said second operation performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce a result of said third operation as said plaintext block i, and

wherein said first circuit performs the first operation on said ciphertext block i and a result of said second operation performed on said ciphertext block i-1, and

wherein either said first random number or said second random number, which is generated by said random number generation circuit, is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation.

~~a circuit for outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back for use in the operation on another one of the plurality of ciphertext blocks; and~~

~~a decryption operation circuit for performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.~~

22. (currently amended) The symmetric-key decryption apparatus as claimed in claim 21, wherein said random number generation circuit divides a

random number sequence longer than said series of ciphertext blocks to produce the random number blocks independent of any one of said ciphertext blocks~~decryption operation circuit uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks~~.

23. (original) The symmetric-key decryption apparatus as claimed in claim 22, further comprising:

a circuit for concatenating a plurality of said plaintext blocks to generate plaintext;

a circuit for extracting redundancy data included in said plaintext; and

a circuit for checking said redundancy data to detect whether said ciphertext has been altered.

24. (currently amended) The symmetric-key decryption apparatus as claimed in claim 23, further comprising:

a circuit for extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key,

wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data~~ to detect whether said ciphertext has been altered~~.

Claims 25-32 (canceled).

33. (currently amended)A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said program when executed causes said computer to performsymmetric-key decryption method comprising the steps of:

~~receiving~~ dividing ciphertext, which is an input text, ~~and dividing the received ciphertext~~ to generate a plurality of ciphertext blocks each having a predetermined length;

~~receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and~~ generating a first random number block and a second random number block both corresponding to each ~~one~~ of said plurality of ciphertext blocks based on a secret key that is an input value~~from said random number sequence~~;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating the series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the ciphertext obtained from the plaintext has been altered,

wherein one of said decryption operations for producing the plaintext block i corresponding to the ciphertext block i (2 <i< a number of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i; and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number of said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

~~outputting a feedback value obtained as a result of operation on said one of said plurality of ciphertext blocks and said random number block, said feedback value being fed back for use in the operation on another one of said plurality of ciphertext blocks; and~~

~~performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and said feedback value obtained as a result of operation on still another one of said plurality of ciphertext blocks to produce a plaintext block.~~

34. (currently amended) The medium storing a program as claimed in claim 33, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said ciphertext block~~said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks~~.

35. (original) The medium storing a program as claimed in claim 34, wherein said symmetric-key decryption method further comprises steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

36. (currently amended) The medium storing a program as claimed in claim 35, wherein said symmetric-key decryption method further comprises steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claim 37 (canceled).

38. (new) The symmetric-key decryption apparatus as claimed in claim 22, wherein said random number generation circuit further comprises:

a pseudorandom number generator for generating said random number sequence based on said secret key; and

a circuit for producing said random number blocks from said random number sequence.